

## A proof that e is transcendental

Jonathan L.F. King

University of Florida, Gainesville FL 32611-2082, USA  
squash@ufl.edu

Webpage <http://www.math.ufl.edu/~squash/>

8 July, 2012 (at 20:28)

**ABSTRACT:** Uses calculus and divisibility to show that e is not algebraic. The file has two proofs, a short one due to Hilbert and a long one, probably of Hermite.

**Notation.** For posint  $N$ , let  $\equiv_N$  means “mod- $N$  congruent”. Let  $::_N::$  mean  $\equiv_{N!}$  i.e., congruence mod  $N$ -factorial.

**1: Lemma.** For  $k$  a natnum, integral  $J_k := \int_0^\infty x^k e^{-x} dx$  equals

$$J_k = k!. \quad \diamond$$

**Proof.** IByParts yields  $J_n = n \cdot J_{n-1}$ . And  $J_0 = 1$ .  $\diamond$

**2: Corollary.** For each natnum  $M$  and intpoly  $f$ :

$$\int_0^\infty f(x) \cdot x^M e^{-x} dx \quad ::_{M+1}:: \quad f(0) \cdot M!.$$

$$\text{Thus } \int_0^\infty f(x) \cdot x^M e^{-x} dx \quad ::_M:: \quad 0. \quad \diamond$$

---

### Hilbert's proof that e is transcendental

**The Set-up.** FTSOC, suppose e is algebraic of degree  $D \in \mathbb{Z}_+$ . We thus have an intpoly

$$h(x) := B_D x^D + \dots + B_1 x + B_0, \text{ with } B_D \neq 0,$$

such that  $h(e) = 0$ . And  $B_0 \neq 0$ , since  $h()$  has minimal degree.  $\square$

**Proof of transcendentality.** For a posint exponent  $r$  to be chosen later, define

$$\Phi(x) := [x-1][x-2][x-3] \cdots [x-D], \quad \text{and}$$

$$\mathbf{I}_\ell^u := \int_\ell^u x^r [\Phi(x)]^{r+1} e^{-x} dx.$$

Thus  $0 = 0 \cdot \mathbf{I}_0^\infty = h(e) \cdot \mathbf{I}_0^\infty = U(r) + L(r)$  where we have split each integral into an Upper part and a Lower part:

$$U(r) := B_0 \mathbf{I}_0^\infty + \sum_{K=1}^D B_K e^K \mathbf{I}_K^\infty, \quad \text{and}$$

$$L(r) := \sum_{K=1}^D B_K e^K \mathbf{I}_0^K.$$

Since  $U(r) + L(r) = 0$ , we have that

$$\frac{U(r)}{r!} + \frac{L(r)}{r!} = 0.$$

The contradiction will come by showing that  $\frac{U(r)}{r!}$  is always a non-zero integer; then showing that  $r$  can be chosen large enough that  $\left| \frac{L(r)}{r!} \right|$  is less than 1.

**Upperbounding  $L(r)$ .** Over all  $x$  in the compact interval  $[0, D]$ , let  $\mathbf{A}$  be an upperbnd for the abs-value of  $x \cdot \Phi(x)$  and of  $\Phi(x)$ . So

$$|x^r \Phi(x)^{r+1} e^{-x}| \leq \mathbf{A}^r \mathbf{A} \cdot 1 = \mathbf{A}^{r+1}.$$

For  $K \in [1..D]$ , then,  $|\mathbf{I}_0^K|$  is bounded by  $D \mathbf{A}^{r+1}$ .

Let  $\mathbf{B} := \sum_{K=1}^D |B_K| \cdot e^K$ . It follows that

$$|L(r)| \leq D \cdot \mathbf{B} \mathbf{A}^{r+1}.$$

Divided by  $r!$ , this quantity goes to zero as  $r \nearrow \infty$ .

**Value  $U(r)$  is a non-zero multiple of  $r!$ .** Fix a  $K \in [1..D]$ . Consider Change-of-Var  $y := x - K$ . Then  $dx = dy$ , and  $e^K \cdot e^{-x} = e^{-y}$ . So  $e^K \cdot \mathbf{I}_K^\infty$  equals

$$*: \int_0^\infty [y+K]^r [y+K-1][y+K-2] \cdots [y+K-D]^{r+1} e^{-y} dy.$$

For  $K \in [1..D]$ , the  $K^{\text{th}}$ -term is  $[y+K-K]$ . Consequently

$$e^K \cdot \mathbf{I}_K^\infty = \int_0^\infty f_K(y) \cdot y^{r+1} e^{-y} dy,$$

for some intpoly  $f_K$ . Hence

$$\dagger: \quad e^K \cdot \mathbf{I}_K^\infty \quad ::_{r+1}:: \quad 0,$$

by setting  $M := r+1$  in (2Lower).

For  $K = 0$ , integral  $\mathbf{I}_0^\infty$  has form  $\int_0^\infty f(x) \cdot x^r e^{-x} dx$ , where  $f(x) := [\Phi(x)]^{r+1}$ . By (2Upper), then,

$$\ddagger: \quad \mathbf{I}_0^\infty \quad ::_{r+1}:: \quad f(0) \cdot r! = [[-1]^D \cdot D!]^{r+1} \cdot r!.$$

Adding up  $B_K \cdot e^K \mathbf{I}_K^\infty$  over all  $K \in [0..D]$  gives, courtesy ( $\dagger, \ddagger$ ), that  $\frac{U(r)}{r!}$  is an integer. Moreover,

$$\frac{U(r)}{r!} \equiv_{[r+1]} B_0 \cdot [[-1]^D \cdot D!]^{r+1}.$$

The righthand quantity is not zero, so integer  $\frac{U(r)}{r!}$  is not zero.  $\diamond$

*Credit.* The following proof may be due to Hermite. I found several versions on the web.  $\square$

**Preliminaries.** For a poly(nomial)  $\mathbf{H}$ , I use  $\text{Dim}(\mathbf{H})$  for  $1 + \text{Deg}(\mathbf{H})$ ; this is the dimension of the vector-space obtained by varying the coefficients of  $\mathbf{H}$ .

Next<sup>♡1</sup> a few lemmata, then to the details. Use  $\binom{7}{2,5}$  for the binomial coeff; it equals  $\frac{7!}{2! \cdot 5!}$ .

**3: Lemma.** For  $\ell$ -times diff'able fncs  $f$  and  $g$ , the  $\ell^{\text{th}}$ -derivative of their product is

$$3': \quad [f \cdot g]^{(\ell)} = \sum_{j+k=\ell} f^{(j)} \cdot g^{(k)} \cdot \binom{\ell}{j,k},$$

where the sum is taken over natnums  $j$  and  $k$ .  $\diamond$

**4: Prop'n.** Fix an integer  $T$  and natnum  $Q$ . Let

$$\mathbf{H}(x) := [x - T]^Q \cdot g(x),$$

where  $g()$  is an intpoly. Differentiating,

$$\begin{aligned} \text{a: } \quad \forall \ell \in [0..Q) : \quad & \mathbf{H}^{(\ell)}(T) = 0. \\ \text{b: } \quad \forall \ell \in \mathbb{N} : \quad & \mathbf{H}^{(\ell)}(T) \blacktriangleright Q!. \\ \text{c: } \quad & \mathbf{H}^{(Q)}(T) = Q! \cdot g(T). \end{aligned}$$

If  $g(x) = \gamma(x)^{Q+1}$ , with  $\gamma$  an intpoly, then

$$\text{d: } \quad \forall \ell \in \mathbb{N} \setminus \{Q\} : \quad \mathbf{H}^{(\ell)}(T) \blacktriangleright [Q+1]!. \quad \diamond$$

*Proof.* Let  $f(x) := [x - T]^Q$ . For each natnum  $j \neq Q$ , note,  $f^{(j)}(T)$  is zero. So (3') yields (4a).

Hence expression  $[f \cdot g]^{(\ell)}(T)$  can be non-zero only when  $\ell \geq Q$ . And  $f^{(Q)}(T) = Q!$ , so by (3'),

$$*: \quad [f \cdot g]^{(\ell)}(T) = Q! \cdot g^{(\ell-Q)}(T) \cdot \binom{\ell}{Q, \ell-Q}.$$

But  $g^{(\ell-Q)}$  is an intpoly, so  $g^{(\ell-Q)}(T)$  is an integer. Thus (4b). Setting  $\ell := Q$  in (\*) gives (4c).

<sup>♡1</sup>Use  $\equiv_N$  to mean "congruent mod  $N$ ". Let  $n \perp k$  mean that  $n$  and  $k$  are co-prime. Use  $k \blacktriangleright n$  for " $k$  divides  $n$ ". Its negation  $k \blacktriangleright n$  means " $k$  does not divide  $n$ ." Use  $n \blacktriangleright k$  and  $n \blacktriangleright k$  for " $n$  is/is-not a multiple of  $k$ ." Finally, for  $p$  a prime and  $E$  a natnum: Use double-verticals,  $p^E \blacktriangleright n$ , to mean that  $E$  is the *highest* power of  $p$  which divides  $n$ . Or write  $n \blacktriangleright p^E$  to emphasize that this is an assertion about  $n$ . Use **PoT** for Power of Two and **PoP** for Power of (a) Prime.

As for (4d), WLOG  $\ell \geq Q+1$  (by (4a)). Note that  $g'(x)$  equals  $[Q+1]$  times some intpoly. (We don't need to know that the intpoly is  $\gamma^Q \cdot \gamma'$ .) So

$$\forall k \geq 1 : \quad g^{(k)}(T) \blacktriangleright Q+1;$$

this used that  $T$  is an integer. Finally, (\*) implies

$$\mathbf{H}^{(\ell)}(T) \blacktriangleright Q! \cdot g^{(k)}(T),$$

where  $k := \ell - Q$ . Together with the preceding line, this implies (4d).  $\blacklozenge$

**5: Trick Lemma.** Consider a poly  $\mathbf{H}()$  and real number  $T \geq 0$ . Let

$$6: \quad \langle T, \mathbf{H} \rangle := \int_0^T [-e^{T-x}] \cdot \mathbf{H}(x) \cdot dx.$$

Letting  $N := \text{Dim}(\mathbf{H})$ , then,

$$7: \quad \langle T, \mathbf{H} \rangle = \left[ \sum_{\ell \in [0..N)} \mathbf{H}^{(\ell)}(T) \right] - e^T \cdot Z,$$

where  $Z := \sum_{\ell \in [0..N)} \mathbf{H}^{(\ell)}(0)$ . If  $T \in \mathbb{N}$  and  $\mathbf{H}()$  is an intpoly, then  $\langle T, \mathbf{H} \rangle$  is an integer. Note that  $Z$  does not depend on  $T$ .  $\diamond$

*Proof.* Integrating by-parts, our  $\langle T, \mathbf{H} \rangle$  equals

$$\begin{aligned} & [e^{T-x}] \cdot \mathbf{H}(x) \Big|_{x=0}^{x=T} - \int_0^T [e^{T-x}] \cdot \mathbf{H}'(x) \cdot dx \\ & = [\mathbf{H}(T) - e^T \mathbf{H}(0)] + \langle T, \mathbf{H}' \rangle. \end{aligned}$$

Using this recurrence  $N$  times gives

$$\langle T, \mathbf{H} \rangle = \text{RhS}(7) + \langle T, \mathbf{H}^{(N)} \rangle.$$

But  $\mathbf{H}^{(N)} \equiv 0$ , so integral  $\langle T, \mathbf{H}^{(N)} \rangle$  is zero.  $\blacklozenge$

**Sequence-properties.** Below, "sequence" will mean a sequence of integers *indexed by the primes*, e.g  $\vec{V} = (V_2, V_3, V_5, V_7, V_{11}, \dots, V_p, \dots)$ .

Say that a  $\vec{V}$  is *slow* if there exist posreals  $\alpha$  and  $\beta$  with

$$\text{S1:} \quad |V_p| \leq \alpha \cdot \beta^p$$

for all large primes  $p$ . Evidently:

‡: A finite linear-combination of slow sequences, is slow.

The argument for transcendence of  $e$  will produce a slow sequence  $\vec{V}$ . On the other hand, were  $e$  algebraic then each  $V_p$  would be an integer with

S2:  $V_p \bullet [p-1]!$ , yet

S3:  $V_p \nmid p$ .

Together (S2,S3) imply that  $|V_p| \geq [p-1]!$ . But this contradicts (S1), seen by sending  $p \nearrow \infty$ .

**The Proof**

8: Theorem (Hermite).  $e$  is transcendental. ◇

*Proof.* FTSOContradiction, suppose  $e$  is algebraic of, say, degree 5. Thus

9: 
$$\sum_{T \in [0..6)} C_T \cdot e^T = 0,$$

for some integers  $C_0, \dots, C_5$ , with  $C_0 \neq 0$ .

A dim= $N$  intpoly  $\mathbf{H}()$  yields an integer

A1: 
$$V := \sum_{T \in [0..6)} C_T \cdot \langle T, \mathbf{H} \rangle.$$

Courtesy (7) and (9),

A2: 
$$V = \sum_{T \in [0..6)} C_T \cdot \sum_{\ell \in [0..N)} \mathbf{H}^{(\ell)}(T).$$

We now choose a particular poly  $\mathbf{H}()$ .

**Slownessitude (S1).** Each prime  $p$  determines a polynomial

10: 
$$\begin{aligned} \mathbf{H}(x) &:= \mathbf{H}_p(x) \\ &:= [x-0]^{p-1} \cdot [x-1][x-2] \dots [x-5]^p. \end{aligned}$$

For each real  $x \in [0, 5]$ , certainly

$$|\mathbf{H}(x)| \leq 5^{p-1} \cdot [5 \dots 5]^p \stackrel{\text{note}}{\leq} [5^6]^p.$$

To upperbound  $\boxed{V_p := V_{\mathbf{H}_p}}$ , it suffices to upperbound  $\langle T, \mathbf{H}_p \rangle$ . Each  $T \in [0..5]$  gives

$$\begin{aligned} |\langle T, \mathbf{H}_p \rangle| &\leq \int_0^T | -e^{T-x} | \cdot |\mathbf{H}(x)| \cdot dx \\ &\leq \int_0^5 e^5 \cdot |\mathbf{H}(x)| \cdot dx. \end{aligned}$$

So  $|\langle T, \mathbf{H}_p \rangle| \leq 5 \cdot e^5 \cdot [5^6]^p$ . Hence  $p \mapsto \langle T, \mathbf{H}_p \rangle$  is slow. The linear combination (A1), then, is slow; i.e  $p \mapsto V_p$  is slow. We have (S1).

For the next two arguments, fix a prime

$$p > \text{Max}(5, |C_0|)$$

and prepare to apply Lemma 4 with  $\boxed{Q := p-1}$ .

**Divisibility (S2).** Each integer  $T \in [0..5]$  is a zero of  $\mathbf{H}()$  with multiplicity at least  $p-1$ . For each natnum  $\ell$ , then,

$$\mathbf{H}^{(\ell)}(T) \bullet [p-1]!,$$

from (4b). So (A2) implies (S2).

**Lack of Divisibility (S3).** For integers  $B$  and  $B'$ , use  $B \bowtie B'$  to mean:

*Either both  $B$  and  $B'$  are divisible by  $p$ , or neither is.*

For  $T = 1, \dots, 5$ , lemma (4b) yields that each  $\mathbf{H}^{(\ell)}(T)$  is divisible by  $p!$ , hence by  $p$ . Thus

$$V \bowtie C_0 \cdot \sum_{\ell \in [0..N)} \mathbf{H}^{(\ell)}(0).$$

By hypothesis,  $0 < |C_0| < p$ . Since  $p$  is prime,

$$V \bowtie \sum_{\ell \in [0..N)} \mathbf{H}^{(\ell)}(0).$$

Using (10), the definition

$$\gamma(x) := [x-1][x-2] \dots [x-5]$$

shows that  $\mathbf{H}()$  has the correct form for lemma (4d). Thus  $V \bowtie \mathbf{H}^{(p-1)}(0)$ . Using (4c) with  $Q := p-1$  and  $T := 0$  gives

$$V \bowtie g(0) \stackrel{\text{note}}{=} \gamma(0)^p.$$

Hence  $V \bowtie \gamma(0)$ . And  $\gamma(0) \bowtie 5!$ . But  $5! \nmid p$ , since prime  $p$  was chosen to exceed the degree, 5, of  $e$ 's purported minimal-polynomial. ◇

Filename: Problems/NumberTheory/e\_transcendental.latex  
As of: Tuesday 24Feb2004. Typeset: 8Jul2012 at 20:28.